

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A method of creating a certificate revocation list (CRL), comprising:
 - a) creating a single CRL that is centralized, said single CRL associated with a single certificate authority (CA) comprising a master server coupled to a plurality of CA clone servers;
 - b) maintaining said single CRL with said master server;
 - c) receiving notice, from one of said plurality of CA clone servers, at said master server containing revocation information regarding a certificate, wherein the one of said plurality of CA clone servers stores the notice in memory; [[and]]
 - d) updating said single CRL according to said revocation information;
 - e) sending notification to the one of said plurality of CA clone servers that the single CRL has been successfully updated; and
 - f) removing the notice comprising the revocation information from the memory of the one of the plurality of CA clone servers upon receipt of the notification.
2. (Original) The method of creating a CRL as described in Claim 1, wherein step d) comprises:
adding said certificate to said single CRL when said revocation information indicates said certificate is revoked, said revocation information associated with a revocation event occurring at one of said plurality of CA clone servers.
3. (Original) The method of creating a CRL as described in Claim 1, wherein step d) comprises:
removing said certificate from said single CRL when said revocation information indicates said certificate is valid, said revocation information associated with a revocation event occurring at one of said plurality of CA clone servers.
4. (Original) The method of creating a CRL as described in Claim 1, further comprising:
maintaining said single CRL with a CRL merger service module located at said master server.

5. (Original) The method of creating a CRL as described in Claim 1, further comprising:
sending said notice over a secure communications channel.
6. (Previously Presented) The method of creating a CRL as described in Claim 5, further comprising:
at said one of said plurality of CA clone servers, performing secure sockets layer (SSL) client authentication over said secure communications channel before sending said notice over said secure communications channel.
7. (Original) The method of creating a CRL as described in Claim 1, further comprising:
transmitting said single CRL that is updated to a recipient over a communication network.
8. (Original) The method of creating a CRL as described in Claim 1, further comprising:
providing certificate authority services not including maintaining and managing said single CRL at each of said plurality of CA clone servers.
9. (Original) The method of creating a CRL as described in Claim 1, further comprising:
storing said CRL in a database accessed via a lightweight directory access protocol (LDAP) that supports a Secure Sockets Layer (SSL).
10. (Original) The method of creating a CRL as described in Claim 1, further comprising:
at said one of said plurality of clone servers, detecting whether said notice was received at said master server;
repeatedly sending notice until received by said master server.
11. (Original) The method of creating a CRL as described in claim 10, further comprising:
storing said notice if said notice was not received at said master server.
12. (Cancelled)
13. (Cancelled)
14. (Cancelled)

15. (Cancelled)

16. (Currently Amended) A single certificate authority (CA) comprising:

a plurality of clone servers coupled together for providing certificate authority services,
wherein each of the plurality of clone servers is configured to store a notice comprising revocation information in memory until a notification is received from the master server that indicates a single CRL has been updated with the revocation information;

[[a]] the single, centralized certificate revocation list (CRL) associated with said CA; and

[[a]] the master server coupled to said plurality of clone servers for maintaining said centralized CRL based on revocation information from said plurality of clone servers,
wherein the master server is configured to send the notification indicating successful updating of the single CRL using the revocation information to the appropriate one of the plurality of clone servers that sent the notice comprising the revocation information.

17. (Original) The CA as described in Claim 16, wherein said master server adds a certificate to said centralized CRL after said revocation information by one of said plurality of clone servers indicates that said certificate has been revoked.

18. (Original) The CA as described in Claim 16, wherein said master server removes a certificate from said centralized CRL after said revocation information by one of said plurality of clone serves indicates that said certificate is valid.

19. (Original) The CA as described in Claim 16, further comprising:

a secure communication network coupling each of said plurality of clone servers to said master server for providing secure communication when said information is sent between said plurality of clone servers and said master server.

20. (Original) The CA as described in Claim 16, further comprising:

a lightweight directory access protocol (LDAP) database that is coupled to said master server for storing said centralized CRL.

21. (Original) The CA as described in Claim 16, further comprising:
a CRL merger service module located at said master server for maintaining said CRL.
22. (Cancelled)
23. (Cancelled)
24. (Cancelled)